EV316936910 103

OCT 2 4 2003 IPE JC37 PATENT & TRADEMARK OFFICE

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Application Serial No. 09/274,294
Filing Date 03/22/1999
Inventorship ....Gunter et al.
Assignee ....Microsoft Corporation
Group Art Unit 2131
Examiner ....Taghi T. Arani
Attorney's Docket No. MS1-298US
Title: System and Method for Trusted Inspection of a Data Stream

5S #12 11/6/03

RECEIVED
OCT 3 0 2003
Technology Center 2100

APPEAL BRIEF

To: Board of Patent Appeals and Interferences
Washington, D.C. 20231

From: Emmanuel A. Rivera (Tel. 509-324-9256; Fax 509-323-8979)
Lee & Hayes, PLLC
421 W. Riverside Avenue, Suite 500
Spokane, WA 99201

Pursuant to 37 C.F.R. §1.192, Appellant hereby submits an appeal brief for application 09/274,294. A Notice of Appeal was filed July 25, 2003. Accordingly, Appellant appeals to the Board of Patent Appeals and Interferences seeking review of the Examiner's rejections.

~~10/29/2003 AWONDAF1 00000132 120769 09274294~~
~~01 FC:1402 330.00 DA~~

10/29/2003 AWONDAF1 00000133 120769 09274294
01 FC:1402 330.00 DA

TABLE OF CONTENTS

(1) Real Party in Interest

The real party in interest is the Microsoft Corporation, the assignee of all right and title to the subject invention.

(2) Related Appeals and Interferences

Appellant is not aware of any other appeals or interferences which will directly affect, be directly affected by, or otherwise have a bearing on the Board's decision to this pending appeal.

(3) Status of Claims

Claims 1-20 were originally submitted. Claims 3, 7, and 12-19 were amended. Claims 1-20 stand rejected and are pending in this Application. All pending claims are set forth in the Appendix of Appealed Claims on page 21.

Claims 1 and 4 stand rejected under 35 U.S.C. §102 as being anticipated by U.S. Patent 5,835,726 to Shwed et al (hereinafter, "Shwed"). Applicants respectfully traverse the rejection.

Claims 2, 3 and 5-20 stand rejected under 35 U.S.C. §103 as being unpatentable over Shwed in view of Bruce Schneier, Applied Cryptography, Second Addition, 1996 (hereinafter, "Schneier").

(4) Status of Amendments

All amendments have been entered, and are reflected in the Appendix of Appealed Claims.

(5) Summary of Invention

The invention concerns a system and method in which two endpoints, also known as clients, communicate via a virtual private network (VPN) on an otherwise public network, such as the Internet, and an intermediary, such as a firewall, is permitted to inspect the data communication in a secure and trusted manner. Each of the clients is able to encrypt data and is part of a network architecture. In one example, an internal client is coupled to the network architecture via an access point, such as a firewall or proxy server. A second, external client is coupled to the access point through the public network. The three participants (internal client, access point, and external client), each have their own pair of public/private keys. An independent key server holds the public keys for all three participants.

The external and internal clients establish a virtual private network with one another by negotiating a session key used to encrypt data being exchanged between them. Initially, only the clients know the session key, and not the access point (firewall). To grant the firewall trusted access to the data stream on the VPN, the internal client securely transfers the session key to the firewall. The internal client requests and receives the firewall's public key from the key server and encrypts the session key using the firewall's public key. The internal client then signs the encrypted key by encrypting it using the internal client's private key.

The firewall authenticates the signature by decrypting the message using the internal client's public key (obtained from the key server or directly from the internal computer). The firewall then decrypts the session key using its own private key. If the dual decryption yields a valid key, the firewall is assured that

the session key was sent by the internal client and was not subsequently altered or tampered with in route.

Once the session key is transferred, the firewall is able to decrypt the data stream on the VPN. The firewall can now un-intrusively inspect the data stream in a manner that is transparent to the external and internal clients. The claims capture this architecture and new technology.

Fig. 2 of the present application is representative of the invention and is reproduced below.

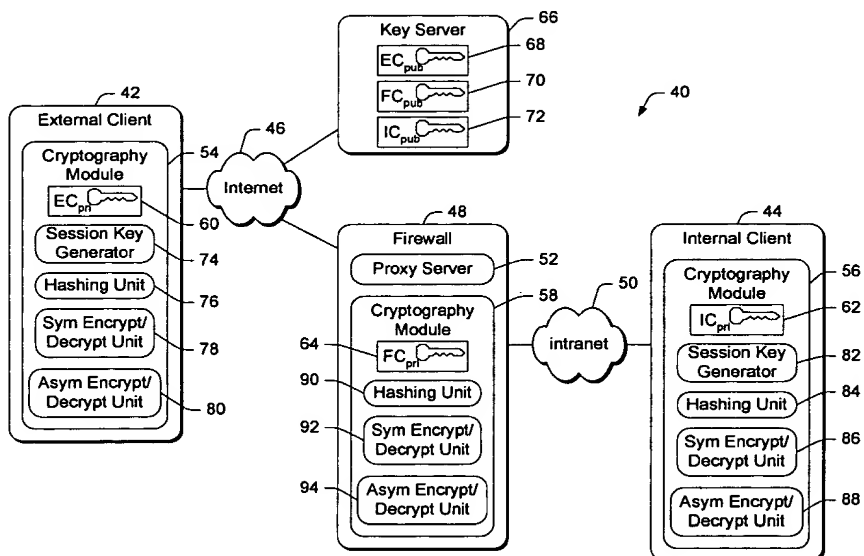

Fig. 2

Fig. 2 shows a network architecture 40 that includes an internal client 44, and external client 42, and an access point or firewall 48. The internal client 44 and the external client 42 employ a VPN through the Internet 46 to communicate with one another. Data may be communicated through firewall 48, which is connected to the external client 42 through the Internet 46 and to the internal client 44 through an intranet 50. See specification page 7, lines 2-8.

External client 42 is equipped with cryptography module 54; internal client 44 is equipped with cryptography module 56; and firewall 48 is equipped with cryptography module 58. The cryptography modules 54, 56, and 58 enable various cryptographic functionality, including encryption, decryption, hashing, authentication, and signing. All three participants also have their own respective pairs of public/private keys. The private keys are stored at the respective participants, as represented by external client private key (EC_{pri}) 60 at external client 42, internal client private key (IC_{pri}) 62 at internal client 44, and firewall computer private key (FC_{pri}) 64 at firewall 48. See specification page 7, lines 11-18.

An independent key server 66 holds corresponding public keys 68, 70, and 72 for external client 42, internal client 44, and firewall 48, respectively. See specification page 7, lines 19-20.

The external client 42 and internal client 44 establish a VPN by negotiating a session key. See specification page 12, lines 14-15. Once the external and internal clients 44, 42 have selected and communicated a shared session key, they are able to tunnel encrypted data through the Internet 46. See specification page 13, lines 3-5. To allow firewall 48 to inspect the data stream, firewall 48 must know the session key. Internal client 44 is responsible for getting the shared session key to firewall 48 in a secure manner. See specification page 13, lines 5-9.

The internal client 44 receives a public key of firewall 48 either from key server 66 or directly from firewall 48 via intranet 50. With the firewall's public key, the session key may be encrypted, sent to, and decrypted by firewall 48. See specification page 13, lines 10-23. Once the firewall 48 gains possession of the

session key, it can dynamically decrypt and monitor VPN data stream communicated between clients 42 and 44.

(6) Issue

Whether claims 1 and 4 are properly rejected under 35 U.S.C. §102 as being anticipated by Shwed.

Whether claims 2, 3 and 5-20 are properly rejected under 35 U.S.C. §103 as being unpatentable over Shwed in view of Schneier.

(7) Grouping of Claims

Appellant respectfully submits that the rejected claims 1-20 do not stand or fall together. The set of pending claims are separated into two groupings of claims. As is explained below, the groupings of the claims are separately patentable. However, it should be understood that the claim groupings below are presented for the purposes of isolating and reducing issues for this Appeal; thus, the claim groupings below should not be considered as the only groupings nor should individual claims be considered as consequentially not separately patentable.

A. Claims 1, 4

B. Claims 2, 3, 5-20

(8) Argument

All of the submitted claims were rejected in the Office Action of 02/04/03 based upon two references: Patent 5,835,726 to Shwed et al (hereinafter, "Shwed") and Bruce Schneier, Applied Cryptography, Second Addition, 1996 (hereinafter, "Schneier").

Shwed describes controlling inbound and outbound data packet flow in a computer network, wherein the data packet flow between two host or client computers may be encrypted by firewalls configured to each of the client computers.

The client computers rely on the firewalls to perform the encryption of data exchanged between the client computers. The firewalls exchange encrypted secure data with one another through a public network such as the Internet. Encrypted data received by a firewall is decrypted, and the decrypted (non-secure) data is passed on to a client computer.

Unlike Appellant's system, the two host or client computers disclosed in Shwed do not perform encryption and do no establish a direct VPN to one another. The system disclosed in Shwed relies on intermediary access points or firewalls to perform encryption and data exchange. The host or client computers communicate (exchange data) through their respective firewalls, and do not directly communicate with another. Furthermore, unlike the Appellant's system, the client or host computers are always aware of the firewalls since the firewalls are an integral part of communication or data exchange.

Fig. 16 of Shwed is redrawn below.

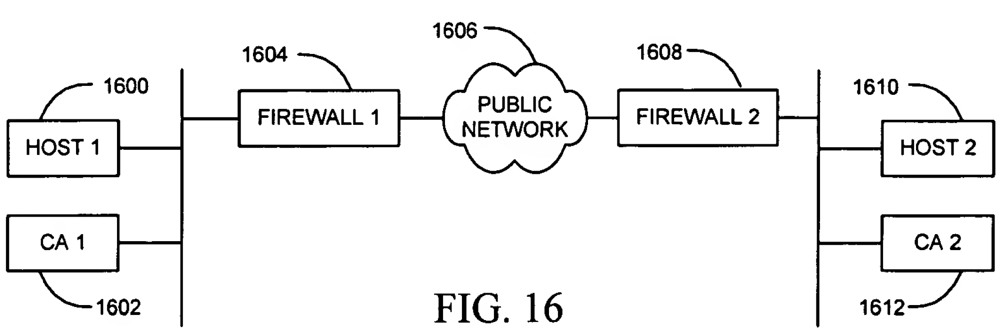

FIG. 16

A host computer "Host 1" 1600 is coupled to a "Firewall 1" 1604; and a host computer "Host 2" is coupled to a "Firewall 2" 1608. A certificate authority (CA) generates a certificate for a public key that can be verified by a recipient host or a firewall. Fig. 16 shows two distinct CA's; "CA 1" 1602 configured to "Host 1" 1600 and "Firewall 1" 1604, and "CA 2" 1612 configured to "Host 2" 1610 and "Firewall 2" 1608. Firewalls 1604 and 1608 are connected to one another by public network 1606 (i.e., the Internet).

Communications from "Host 1" 1600 is routed to the public network 1606 via "Firewall 1" 1604 which acts as a firewalled network object. Similarly, communications from "Host 2" 1610 is routed to the public network 1606 via "Firewall 2" 1608 which also acts as a firewalled network object. "Firewall 1" 1604 intercepts and encrypts data packets it receives from "Host 1" 1600 destined for "Host 2" 1610. "Firewall 2" 1608 receives the encrypted data packets destined for "Host 2" 1610 and decrypts those data packets and passes them to "Host 2" 1610. In the opposite direction, "Firewall 2" 1608 encrypts data packets from "Host 2" 1610 destined for "Host 1" 1600. "Firewall 1" 1604 receives the encrypted data packets destined for "Host 1" 1600, decrypts them and passes them to "Host 1" 1600.

If "Host 1" 1600 initiates a session with "Host 2" 1610, it sends an non-encrypted Internet Protocol (IP) packet to "Host 2" 1610. "Firewall 1" 1604 intercepts the non-encrypted IP packet and determines that communications between "Host 1" 1600 and "Host 2" are to be modified in some way (e.g., encryption, decryption, address translation). If determination is made that communications between "Host 1" 1600 and "Host 2" 1610 are to be encrypted or

digitally signed, "Firewall 1" 1604 temporarily parks the non-encrypted IP packet and initiates a session key exchange with "Firewall 2" 1608.

Before encrypted communications or signing can take place, firewalls 1604 and 1608 agree on a shared key, or session key, which is generated at the start of every session. Only the communications between firewalls 1604 and 1608 is encrypted. The communications between "Host 1" 1600 and "Firewall 1" 1604 and between "Host 2" 1610 and "Firewall 2" 1608 are not encrypted because it takes place over private local area networks (LAN) that are assumed to be private and secure.

The secondary reference, Schneier, is cited for its teaching of known cryptosystems, in particular key exchange systems. Schneier is a well-known book, and is referenced on page 6 of the subject application. Schneier is particularly cited for teaching a hybrid cryptosystem where public-key cryptography is used to secure and to distribute a session key; and the use of a digital signature to (i.e., signing a message/data stream or document) with public key cryptography.

The following arguments are organized into two sub-arguments, one for each of the claim groupings.

(1) **The Cited Reference of Shwed Does Not Disclose An Encrypted Datastream Transferred Between Two Endpoints**

All claims in grouping *A* (claims 1, 4) stand rejected under 35 U.S.C. §102(a) as anticipated by Shwed .

Claim 1 is representative of claim grouping *A*. **Claim 1** recites in part:

> A method for inspecting an encrypted data stream being transferred over a network between two endpoints, the data stream being

> encrypted using a session key known to both endpoints, the method comprising:
>
> securely transferring the session key from one of the endpoints to an intermediary having access to the encrypted data stream;
>
> decrypting the encrypted data stream at the intermediary using the session key …

Shwed does not disclose the environment recited in the preamble; namely, "an encrypted data stream being transferred over a network between two endpoints", where the data stream is "encrypted using a session key known to both endpoints". The endpoints described in Shwed are host or client computers 1600 and 1610. These computers do no directly exchange data (i.e., communicate) with one another. Instead, firewall computers 1604 and 1608 perform encryption and decryption of data exchanged between the host computers to assure the data is protected as it is transferred over a public network.

The Examiner argues that "Shwed desires that the communications between Host 1 and Host 2 be secured" referring to Shwed at col. 14, lines 40-41. However, this security is only performed through firewall 1 and firewall 2. In other words, secured communication disclosed by Shwed is from firewall to firewall, or in other cases a client (host) to a firewall. Shwed states "… only the communication between firewall1 and firewall2 are actually encrypted." (Shwed at col. 15 lines 31-32). Shwed further clarifies "[t]he communications between host1 and firewall1 and between host2 and firewall2 are not encrypted." (Shwed at col. 15 lines 8-10).

Furthermore, Shwed does not disclose that endpoints host 1 and host 2 both know a session key. The Examiner has pointed to teachings in Shwed that show a session key that is known by a firewall or an outside client, but no disclosure of a

session key known to both endpoints. In Shwed, a session key is generated by the non-initiator firewall also called the destination and is sent encrypted to the initiator firewall (Shwed at col. 15, lines 33-35). Shwed does not disclose that either host 1 or host 2 would know the session key. This is understandable because in Shwed's architecture, neither host 1 nor host 2 decrypt or encrypt data. Shwed makes particular mention that communication to and from host 1 and host 2 are never encrypted, and does not disclose that either host 1 or host 2 would know a session key.

Shwed further fails to disclose "securely transferring the session key from one of the endpoints to an intermediary having access to the encrypted data stream". There is no discussion whatsoever with respect to this limitation. Accordingly, the Office renamed the Shwed architecture to call one of the intermediaries or firewalls as an "endpoint". More specifically, the Examiner argues that firewall 1 and firewall 2 may be treated as intermediaries *and/or* as sources (i.e., endpoints). The Examiner argues that "[f]irewall1 is a source of transmitting encrypted packet[s] to intermediary firewall2, while it is also an intermediary point for inspecting packets received from host2." In this arrangement, firewall 1 is an endpoint and host 2 is the other endpoint, and firewall 2 is an intermediary.

However, even given this unintended and forced construction, the structure still does not satisfy the claim limitation. An encrypted data stream is never transferred over the network 1606 between firewall 1 and host 2. Moreover, the host 2 does not securely transfer the session key to the firewall 2.

Accordingly, Shwed does not anticipate claim 1 and the rejection of claim 1 is unfounded. Allowance of claim 1 is respectfully requested.

Claim 4 of Group *A* depends from claim 1, and is allowable because of its dependence from an allowable base claim.

(2) <u>The Cited Combination of Shwed and Schneier Does Not Teach or Suggest An Endpoint Session Key Obtained And Decrypted By An Intermediary</u>

All claims in grouping *B* (claims 2, 3, and 5-20) stand rejected under 35 U.S.C. §103(a) as being unpatentable over Shwed and Schneier.

Claims 2 and 3 depend from claim 1. Accordingly, claims 2 and 3 are allowable at the least for the reasons discussed above with regard to claim grouping *A*.

Furthermore, claims 2 and 3 recite in pertinent part:

> encrypting the session key using a public key associated with the intermediary; and
>
> sending the encrypted session key to the intermediary.

Shwed does not suggest or teach a session key known to both endpoints. The session key in Shwed is known only by and between the intermediary firewalls not the endpoint computers host 1 and host 2. Host 1 and host 2 do not share a common session key nor are they involved in encryption with one another. The Examiner argues that one of the firewalls may be treated as an endpoint, in as much as the firewalls do know a session key. However, in configurations that are taught by Shwed, either host 1 or host 2 is considered an endpoint. Shwed does not does suggest or teach that either host 1 or host 2 as knowing a session key, therefore Shwed fails to teach or suggest the elements of "encrypting the session

key using a public key associated with the intermediary; and sending the encrypted session key to the intermediary".

Schneier is cited for its teaching of known cryptosystems, in particular key exchange systems. Schneier provides no assistance as to the recited methodology of claim 1 from which claims 2 and 3 depend. That is apart from discussing cryptographic ciphers, Schneier provides no teaching of a method for inspecting an encrypted data stream over a network between endpoints when the session key is securely transferred from one of the endpoints to an intermediary.

In this case, the prior art discloses no advantages or utility for the proposed combination. Accordingly, the combination proposed by the Examiner would not have been obvious, and the rejection of claims 2 and 3 is unfounded. Allowance of claims 2 and 3 is respectfully requested.

Claim 5 is representative of claim grouping *B*. Claim 5 is directed generally to an intermediary obtaining and decrypting an endpoint session key known by two endpoints and used to decrypt encrypted data passed between the two endpoints.

Claim 5 recites in pertinent part:

> obtaining, at the intermediary, the one endpoint's public key from the key storage;
>
> decrypting, at the intermediary, the signed encrypted session key using the one endpoint's public key to return the encrypted session key;
>
> decrypting, at the intermediary, the encrypted session key using the intermediary's private key to return the session key

As discussed, the Shwed/Schneier combination does teach or suggest encryption of a data stream between two endpoint computers host 1 and host 2.

The firewalls disclosed in Shwed perform encryption of data between themselves, where initiation of encrypted communication begins with generating a session key between the firewalls. The firewalls pass the session key between themselves. The endpoint computers host 1 and host 2 do not directly exchange encrypted data with themselves. The systems described in Shwed always involve a firewall whenever encrypted communications take place. Either a first firewall and second firewall will exchange the session key, or a first firewall and a personal computer (PC) will exchange. In all scenarios described in Shwed, at least one firewall will be part of the session key generation and exchange, and will always know the session key. Furthermore, the client/firewall key exchange disclosed in Shwed particularly points out that "in firewall to firewall communications, both sides have each other's certified public key. In client to firewall communication, this is only true for the client, while the server [firewall] identifies the client using a name/password pair sent to it by the client". Shwed col. 21, lines 2-7.

The combination of Shwed/Schneier fails to teach or suggest "obtaining, at the intermediary, the one endpoint's public key from the key storage" since Shwed specifically points out that neither a host computer nor a client computer has a public key. Therefore there is no endpoint public key that may be obtained from key storage by the intermediary (firewall).

Furthermore, since the firewalls or intermediaries of Shwed perform the encryption/decryption of the data, they initiate and generate the session key. Because the session key is known to the firewalls of Shwed, it would be counterintuitive to have a firewall or intermediary perform the recited elements of "decrypting, at the intermediary, the signed encrypted session key using the one endpoint's public key to return the encrypted session key" and "decrypting, at the

intermediary, the encrypted session key using the intermediary's private key to return the session key".

In this case, the prior art discloses no advantages or utility for the proposed combination. Accordingly, the combination proposed by the Examiner would not have been obvious, and the rejection of claim 5 is unfounded. Allowance of claim 5 is respectfully requested.

Claim 6 depends from claim 5, and is allowable because of its dependency from an allowable claim.

Claim 7 recites in pertinent part:

> In a network system having an internal client that exchanges encrypted data with an external client over a network and through a firewall intermediate of the internal and external clients, the encrypted data being encrypted using a session key known to the internal and external clients, a method executed at the firewall comprising:
>
> receiving an encrypted and signed session key from the internal client, the encrypted and signed session key bearing a digital signature of the internal client;

As discussed, the Shwed/Schneier combination does not suggest nor teach that an internal client exchange encrypted data with an external client using a session key known to the internal and external clients. Claim 7 further benefits from the arguments presented in support of claim 5, in particular the Shwed/Schneier combination does not suggest nor teach "receiving an encrypted and signed session key from the internal client, the encrypted and signed session key bearing a digital signature of the internal client" at the firewall.

In this case, the prior art discloses no advantages or utility for the proposed combination. Accordingly, the combination proposed by the Examiner would not

have been obvious, and the rejection of claim 7 is unfounded. Allowance of claim 7 is respectfully requested.

Claim 8, 9, 10, and 11 depend from claim 7, and are allowable because of their dependency from an allowable claim.

Claim 12 recites in pertinent part:

A network system comprising:

> an internal client device and an external client device configured to communicate encrypted data over a network using virtual private network communication, the data being encrypted using a session key;
>
> the internal client device being configured to securely transfer the session key to the intermediary device;

Claim 12 benefits from the arguments presented in support of claim 5, in particular the Shwed/Schneier combination does not suggest nor teach "an internal client device and an external client device configured to communicate encrypted data over a network using virtual private network communication" and that "the internal client device being configured to securely transfer the session key to the intermediary device".

In this case, the prior art discloses no advantages or utility for the proposed combination. Accordingly, the combination proposed by the Examiner would not have been obvious, and the rejection of claim 12 is unfounded. Allowance of claim 12 is respectfully requested.

Claim 13, 14, and 15 depend from claim 12, and are allowable because of their dependency from an allowable claim.

Claim 16 recites in pertinent part:

A software architecture for a network system having two endpoints that exchange encrypted data over a network and through an

intermediary, the encrypted data being encrypted using a session key known to the endpoints comprising:

endpoint-resident code stored on computer readable media and executable on a processor to encrypt the session key using a public key from a public/private key pair associated with the intermediary and to sign the encrypted session key with a digital signature, the endpoint-resident code being capable of sending the signed and encrypted session key to the intermediary

Claim 16 benefits from the arguments presented in support of claim 5, in particular the Shwed/Schneier combination does not suggest nor teach "sending the signed and encrypted session key to the intermediary".

In this case, the prior art discloses no advantages or utility for the proposed combination. Accordingly, the combination proposed by the Examiner would not have been obvious, and the rejection of claim 16 is unfounded. Allowance of claim 16 is respectfully requested.

Claim 17 and 18 depend from claim 16, and are allowable because of their dependency from an allowable claim.

Claim 19 recites in pertinent part:

an internal client that exchanges encrypted data with an external client over a network and through a firewall intermediate of the internal and external clients, the encrypted data being encrypted using a session key known to the internal and external clients, computer-readable media distributed at the internal client and the firewall storing computer-executable instructions for:

passing the signed and encrypted session key to the intermediary

Claim 19 benefits from the arguments presented in support of claim 5, in particular the Shwed/Schneier combination does not suggest nor teach "passing the signed and encrypted session key to the intermediary".

In this case, the prior art discloses no advantages or utility for the proposed combination. Accordingly, the combination proposed by the Examiner would not have been obvious, and the rejection of claim 19 is unfounded. Allowance of claim 19 is respectfully requested.

Claim 20 recites in pertinent part:

> In a network system in which an encrypted data stream is transferred over a network between two endpoints and via an intermediary, the data stream being encrypted using a session key known to both endpoints, computer-readable media at one of the endpoints and at the intermediary storing computer-executable instructions for:
>
> securely transferring the session key from one of the endpoints to an intermediary having access to the encrypted data stream

Claim 20 benefits from the arguments presented in support of claim 5, in particular the Shwed/Schneier combination does not suggest nor teach "securely transferring the session key from one of the endpoints to an intermediary having access to the encrypted data stream".

In this case, the prior art discloses no advantages or utility for the proposed combination. Accordingly, the combination proposed by the Examiner would not have been obvious, and the rejection of claim 20 is unfounded. Allowance of claim 20 is respectfully requested.

Conclusion

Appellant respectfully requests that the §102 and §103 rejections be withdrawn and that pending claims 1-20 be allowed.

Respectfully Submitted,

Dated: Oct. 24, 2003

By: Lee C. Lee Reg. No. 34,656
for Emmanuel A. Rivera, Reg. No. 45,760
(509) 324-9256

(9) Appendix of Appealed Claims

1. A method for inspecting an encrypted data stream being transferred over a network between two endpoints, the data stream being encrypted using a session key known to both endpoints, the method comprising:

securely transferring the session key from one of the endpoints to an intermediary having access to the encrypted data stream;

decrypting the encrypted data stream at the intermediary using the session key; and

inspecting the data stream following decryption.

2. A method as recited in claim 1, wherein securely transferring comprises:

encrypting the session key using a public key associated with the intermediary; and

sending the encrypted session key to the intermediary.

3. A method as recited in claim 1, wherein securely transferring comprises:

encrypting the session key using a public key associated with the intermediary;

signing the encrypted session key using a private key associated with the one of the endpoints; and

sending the signed and encrypted session key to the intermediary.

4. A method as recited in claim 1, further comprising storing the data stream at the intermediary.

5. A method for inspecting an encrypted data stream being transferred over a network between two endpoints and via an intermediary, the data stream being encrypted using a session key known to both endpoints, the method comprising:

storing a public key from a public/private key pair associated with one of the endpoints at a key storage;

storing a public key from a public/private key pair associated with the intermediary at the key storage;

obtaining, at said one endpoint, the intermediary's public key from the key storage;

encrypting, at said one endpoint, the session key using the intermediary's public key to produce an encrypted session key;

encrypting, at said one endpoint, the encrypted session key using a private key from the public private key pair associated with said one endpoint to produce a signed encrypted session key;

passing the signed encrypted session key to the intermediary;

obtaining, at the intermediary, the one endpoint's public key from the key storage;

decrypting, at the intermediary, the signed encrypted session key using the one endpoint's public key to return the encrypted session key;

decrypting, at the intermediary, the encrypted session key using the intermediary's private key to return the session key; and

using the session key at the intermediary to decrypt the encrypted data stream.

6. In a network system in which an encrypted data stream is transferred over a network between two endpoints and via an intermediary, the data stream being encrypted using a session key known to both endpoints, computer-readable media at one of the endpoints and at the intermediary storing computer-executable instructions for performing the method as recited in claim 5.

7. In a network system having an internal client that exchanges encrypted data with an external client over a network and through a firewall intermediate of the internal and external clients, the encrypted data being encrypted using a session key known to the internal and external clients, a method executed at the firewall comprising:

receiving an encrypted and signed session key from the internal client, the encrypted and signed session key bearing a digital signature of the internal client;

authenticating the digital signature as belonging to the internal client;

decrypting the session key; and

decrypting the encrypted data being exchanged between the internal and external clients using the session key.

8. A method as recited in claim 7, wherein the encrypted and signed session key is encrypted using a public key from a public/private key pair associated with the firewall, and the decrypting comprises decrypting the session key using a private key from the pubic/private key pair.

9. A method as recited in claim 7, further comprising inspecting the data in an unencrypted form.

10. A method as recited in claim 7, further comprising storing the data in an unencrypted form.

11. In a network system having an external client that exchanges encrypted data with an external client over a network and through a firewall intermediate of the internal and external clients, the encrypted data being encrypted using a session key known to the internal and external clients, a computer-readable medium resident at the firewall storing computer-executable instructions for performing method as recited in claim 7.

12. A network system comprising:

an internal client device and an external client device configured to communicate encrypted data over a network using virtual private network communication, the data being encrypted using a session key;

an intermediary device having access to the encrypted data being communicated between the internal client device and the external client device;

the internal client device being configured to securely transfer the session key to the intermediary device; and

the intermediary device being configured to decrypt the data using the session key and to inspect the data.

13. A network system as recited in claim 12, wherein the internal client device encrypts the session key prior to sending it to the intermediary device.

14. A network system as recited in claim 12, wherein the internal client device encrypts and signs the session key prior to sending it to the intermediary device.

15. A network system as recited in claim 12, wherein the intermediary device stores the data in unencrypted form.

16. A software architecture for a network system having two endpoints that exchange encrypted data over a network and through an intermediary, the encrypted data being encrypted using a session key known to the endpoints, comprising:

endpoint-resident code stored on computer readable media and executable on a processor to encrypt the session key using a public key from a public/private key pair associated with the intermediary and to sign the encrypted session key with a digital signature, the endpoint-resident code being capable of sending the signed and encrypted session key to the intermediary; and

intermediary-resident code stored on computer readable media and executable on the processor to authenticate the digital signature and decrypt the encrypted session key using a private key from the public/private key pair associated with the intermediary, the intermediary-resident code using the session key to decrypt the encrypted data as it is being exchanged between the two endpoints.

17. A software architecture as recited in claim 16, wherein the intermediary-resident code inspects the data in unencrypted form.

18. A software architecture as recited in claim 16, wherein the intermediary-resident code stores the data in unencrypted form.

19. In a network system having an internal client that exchanges encrypted data with an external client over a network and through a firewall intermediate of the internal and external clients, the encrypted data being encrypted using a session key known to the internal and external clients, computer-readable media distributed at the internal client and the firewall storing computer-executable instructions for:

encrypting the session key at the internal client;

signing the encrypted session key with a digital signature associated with the internal client;

passing the signed and encrypted session key to the intermediary;

authenticating, at the intermediary, the digital signature of the internal client;

decrypting the session key at the intermediary;

decrypting, at the intermediary, the encrypted data using the session key; and

inspecting the data in route between the internal and external clients.

20. In a network system in which an encrypted data stream is transferred over a network between two endpoints and via an intermediary, the data stream being encrypted using a session key known to both endpoints, computer-readable media at one of the endpoints and at the intermediary storing computer-executable instructions for:

securely transferring the session key from one of the endpoints to an intermediary having access to the encrypted data stream;

decrypting the encrypted data stream at the intermediary using the session key; and

inspecting the data stream following decryption.